(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－317376
（P2003－317376A）
(43)公開日　平成15年11月７日(2003.11.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｚ	５Ｃ０６４
Ｈ０４Ｎ　7/173	６４０	Ｈ０４Ｎ　7/173	６４０Ａ	５Ｄ０４４

審査請求　未請求　請求項の数７　ＯＬ　（全 17 頁）

(21)出願番号　特願2002－111555(P2002－111555)

(22)出願日　平成14年４月15日(2002.4.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　川本　洋志
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報管理装置および方法、記録媒体、並びにプログラム

(57)【要約】
【課題】　コンテンツの不正な利用を防止する。
【解決手段】　クライアント１のリッピングモジュール９１により、CD８１に記録されているコンテンツが取り込まれ、記憶部２８に保存される。クライアント１においては、コンテンツを識別するコンテンツID（CID）と、クライアント１（リッピングモジュール９１）に対して固有のユニークID（Uniq ID）が生成され、それらのIDが、リッピングモジュール９１により取り込まれたコンテンツに付加される。また、クライアント１においては、コンテンツの使用条件等が記述された利用権が生成され、保存される。利用権には、コンテンツに付加されているユニークIDと同一のIDが設定されている装置（クライアント）のみでのコンテンツの再生を許可することを表す情報が記述される。本発明は、パーソナルコンピュータなどの情報処理装置に適用することができる。

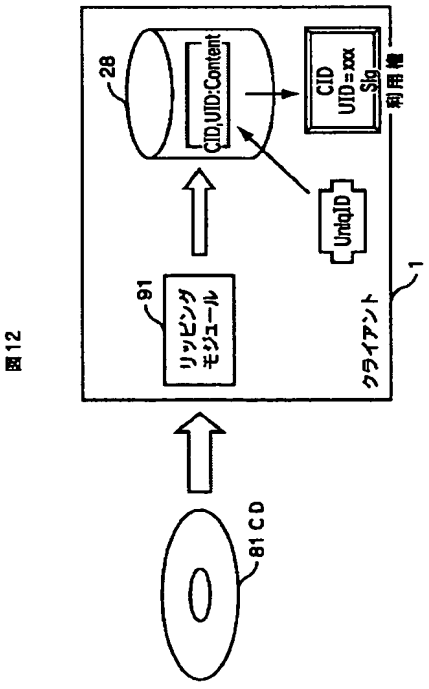


図12

【特許請求の範囲】
【請求項１】　コンテンツを管理する情報管理装置において、前記コンテンツを取得するコンテンツ取得手段と、前記情報管理装置を識別する識別情報を取得する識別情報取得手段と、前記コンテンツ取得手段により取得された前記コンテンツに、前記識別情報取得手段により取得された前記識別情報を付加して記憶するコンテンツ記憶手段と、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶手段とを備えることを特徴とする情報管理装置。
【請求項２】　前記コンテンツに付加されている前記識別情報と、前記識別情報取得手段により取得された前記識別情報が同一であるとき、前記コンテンツを再生する再生手段をさらに備えることを特徴とする請求項１に記載の情報管理装置。
【請求項３】　前記コンテンツ取得手段は、前記情報管理装置に装着された所定の記録媒体から前記コンテンツを取得することを特徴とする請求項１に記載の情報管理装置。
【請求項４】　前記識別情報取得手段は、生成した乱数を前記識別情報とすることを特徴とする請求項１に記載の情報管理装置。
【請求項５】　コンテンツを管理する情報管理装置の情報管理方法において、前記コンテンツを取得するコンテンツ取得ステップと、前記情報管理装置を識別する識別情報を取得する識別情報取得ステップと、前記コンテンツ取得ステップの処理により取得された前記コンテンツに、前記識別情報取得ステップの処理により取得された前記識別情報を付加して記憶するコンテンツ記憶ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶ステップとを含むことを特徴とする情報管理方法。
【請求項６】　コンテンツを管理する情報管理装置の記録媒体において、前記コンテンツの取得を制御するコンテンツ取得制御ステップと、前記情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、前記コンテンツ取得制御ステップの処理により取得された前記コンテンツに、前記識別情報取得制御ステップの処理により取得された前記識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項７】　コンテンツを管理する情報管理装置を制御するコンピュータに、前記コンテンツの取得を制御するコンテンツ取得制御ステップと、前記情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、前記コンテンツ取得制御ステップの処理により取得された前記コンテンツに、前記識別情報取得制御ステップの処理により取得された前記識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップとを実行させるプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報管理装置および方法、記録媒体、並びにプログラムに関し、特に、コンテンツの不正な再生を容易に防止できるようにする情報管理装置および方法、記録媒体、並びにプログラムに関する。
【０００２】
【従来の技術】近年、各種のブロードバンド環境が整備されつつあり、音楽データや動画データなどの各種のコンテンツの配信サービスが本格的に開始され始めている。
【０００３】例えば、「PressPlay（商標）」などの定期購読型（subscription型）の音楽配信サービスが行われており、この音楽配信サービスにおいては、ユーザは、月極の定額の料金を支払うことで、予め設定されている条件の範囲内（例えば、ストリーミング再生の場合１０００曲まで再生可能、ダウンロードしてパーソナルコンピュータのハードディスクに保存する場合１００曲まで保存可能、CD(Compact Disk)-Rへの書き込み（コピー）する場合２０曲までコピー可能などの条件の範囲内）で音楽コンテンツを利用することができる。
【０００４】ところで、このような配信サービスによるコンテンツの提供を受けるユーザの権利情報を管理するシステムとして、例えば、特開平２００１－３５２３２１号公報には、複数のサービスに対応するノードをツリー状に配置してなるシステムにおいて、所定のサービスに対応するノードから、そのサービスに属するそれぞれのリーフのノード（デバイス）までのパス上に存在するノードに設定されている鍵情報（DNK(Device Node Key)）を含む有効化キーブロック（EKB(Enabling Key Block)）を用いることが開示されている。
【０００５】このシステムでは、あるサービスにおいて配信されるコンテンツにEKBが付加されており、個々のデバイスに対して与えられているDNKを利用して、EKBに含まれる、更新された鍵情報を取得させることにより、

サービスの利用を許可するデバイスを管理している。この場合において、DNKを利用して、EKBから、更新された鍵情報を取得できないデバイスは、その後、サービスの提供を受けることができない。

【０００６】そして、これにより、コンテンツを提供するサーバとデバイスとの間で認証処理などをその都度行うことなく、それぞれのデバイスにおけるコンテンツの利用を管理できるようにしたものである。

【０００７】また、このようにしてコンテンツの権利情報が管理されるシステムにおいては、例えば、CD(Compact Disk)からコンテンツをインポートしたデバイスは、そのコンテンツをICV(Integrity Check Value)により管理するようになされている。

【０００８】図１は、インポートしたコンテンツをICVにより管理する構成を模式的に示す図である。

【０００９】図１に示されるように、例えば、パーソナルコンピュータなどのデバイスは、CDからインポートしたコンテンツ（音楽データ）をハードディスクの管理テーブルに登録し、登録されているコンテンツに基づいて生成されたMAC(Message Authentication Code)（Ｃ１，Ｃ２，…，Ｃｎ）をICV＝hash(Ｋｉｃｖ，Ｃ１，Ｃ２，…，Ｃｎ)に適用し、ICVを生成する。なお、ＫｉｃｖはICVを生成するための鍵情報である。

【００１０】そして、コンテンツ生成時に生成し、安全に保存しておいたICVと、再生時などの所定のタイミングで新たに生成したICVとを比較し、同一のICVが得られれば、コンテンツに改竄がなかったと判定され、一方、得られたICVがコンテンツ生成時のものと異なる場合、コンテンツに改竄があったと判定される。コンテンツに改竄がなかったと判定された場合、続けて、コンテンツの再生処理が行われ、改竄があったと判定された場合、再生処理は行われない。従って、これにより、改竄されたコンテンツの再生が防止される。

【００１１】

【発明が解決しようとする課題】しかしながら、以上のようにしてICVによりコンテンツを管理する場合、コンテンツをインポートする毎に、或いはコンテンツを再生する毎にICVを生成しなければならず、その処理負担が大きいという課題があった。

【００１２】従って、音楽再生用デバイスなどのポータブルデバイスにとっては、ICVを生成するためのハッシュ演算が可能な高性能の演算部が必要となり、そのような演算部を設けるようにした場合、結果として、デバイスのコストが上がることとなる。

【００１３】本発明はこのような状況に鑑みてなされたものであり、コンテンツの不正な再生を容易に防止できるようにするものである。

【００１４】

【課題を解決するための手段】本発明の情報管理装置は、コンテンツを取得するコンテンツ取得手段と、情報管理装置を識別する識別情報を取得する識別情報取得手段と、コンテンツ取得手段により取得されたコンテンツに、識別情報取得手段により取得された識別情報を付加して記憶するコンテンツ記憶手段と、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶手段とを備えることを特徴とする。

【００１５】コンテンツを再生する再生手段がさらに設けられ、その再生手段が、コンテンツに付加されている識別情報と、識別情報取得手段により取得された識別情報が同一であるときにのみコンテンツを再生するようにしてもよい。

【００１６】コンテンツ取得手段は、情報管理装置に装着された所定の記録媒体からコンテンツを取得することを特徴とする。

【００１７】識別情報取得手段は、自分自身が生成した乱数を識別情報として、コンテンツ等に付加するようにしてもよい。また、識別情報は外部の装置などから提供されるものであってもよい。

【００１８】本発明の情報管理装置の情報管理方法は、コンテンツを取得するコンテンツ取得ステップと、情報管理装置を識別する識別情報を取得する識別情報取得ステップと、コンテンツ取得ステップの処理により取得されたコンテンツに、識別情報取得ステップの処理により取得された識別情報を付加して記憶するコンテンツ記憶ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶ステップとを含むことを特徴とする。

【００１９】本発明の情報管理装置の記録媒体には、コンテンツの取得を制御するコンテンツ取得制御ステップと、情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、コンテンツ取得制御ステップの処理により取得されたコンテンツに、識別情報取得制御ステップの処理により取得された識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップを、コンピュータに実行させるプログラムが記録されていることを特徴とする。

【００２０】本発明のプログラムは、コンテンツを管理する情報管理装置を制御するコンピュータに、コンテンツの取得を制御するコンテンツ取得制御ステップと、情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、コンテンツ取得制御ステップの処理により取得されたコンテンツに、識別情報取得制御

ステップの処理により取得された識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権情報の記憶を制御する利用権記憶制御ステップとを実行させることを特徴とする。

【００２１】本発明の情報管理装置および方法、並びにプログラムにおいては、コンテンツが取得され、情報管理装置を識別する識別情報が取得される。また、取得されたコンテンツに対して、取得された識別情報が付加されて記憶され、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権が記憶される。

【００２２】

【発明の実施の形態】図２は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット２には、クライアント１－１，１－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１と称する）が接続されている。この例においては、クライアントが２台のみ示されているが、インターネット２には、任意の台数のクライアントが接続される。

【００２３】また、インターネット２には、クライアント１に対してコンテンツを提供するコンテンツサーバ３、コンテンツサーバ３が提供するコンテンツを利用するのに必要な利用権をクライアント１に対して付与するライセンスサーバ４、およびクライアント１が利用権を受け取った場合に、そのクライアント１に対して課金処理を行う課金サーバ５が接続されている。

【００２４】これらのコンテンツサーバ３、ライセンスサーバ４、および課金サーバ５も、任意の台数だけ、インターネット２に接続される。

【００２５】図３はクライアント１の構成を表している。

【００２６】図３において、CPU（Central Processing Unit）２１は、ROM（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からRAM（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をCPU２１に供給する。RAM２３にはまた、CPU２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００２７】暗号化復号部２４は、コンテンツを暗号化するとともに、既に暗号化されているコンテンツを復号する処理を行う。コーデック部２５は、例えば、ATRAC（Adaptive Transform Acoustic Coding）３方式などでコンテンツをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。半導体メモリ４４は、例えば、メモリスティック（商標）などにより構成される。

【００２８】CPU２１、ROM２２、RAM２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

【００２９】入出力インタフェース３２には、キーボード、マウスなどよりなる入力部２６、CRT(Cathode Ray Tube)、LCD(Liquid Crystal Display)などよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、モデム、ターミナルアダプタなどより構成される通信部２９が接続されている。通信部２９は、インターネット２を介しての通信処理を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【００３０】入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

【００３１】なお、図示は省略するが、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５も、図３に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図３の構成は、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５などの構成としても引用される。

【００３２】本発明においては、図４に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイス固有のキーに対応する。本発明のシステムに用いられる階層ツリー構造鍵管理については特開２００１－３５２３２１号公報に記載されている。図４の例の場合、番号０から番号１５までの１６個のデバイスに対応するキーが生成される。

【００３３】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKR（適宜、Ｋｒｏｏｔとも称する）が規定され、２段目のノードに対応してキーＫ０，Ｋ１が規定される。また、３段目のノードに対応してキーＫ００乃至Ｋ１１が規定され、第４段目のノードに対応してキーＫ０００乃至キーＫ１１１が規定される。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーＫ０００乃至Ｋ１１１１が、

それぞれ対応されている。

【００３４】階層構造とされているため、例えば、キーＫ００１０とキーＫ００１１の上位のキーは、Ｋ００１とされ、キーＫ０００とキーＫ００１の上位のキーは、Ｋ００とされている。以下、同様に、キーＫ００とキーＫ０１の上位のキーは、Ｋ０とされ、キーＫ０とキーＫ１の上位のキーは、KRとされている。

【００３５】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの１つのパスの各ノードに対応するキーで管理される。例えば、番号３のリーフに対応するデバイスにおいて、コンテンツを利用するためのキーは、キーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，KRを含むパスの各キーで管理される。

【００３６】本発明のシステムにおいては、図５に示されるように、図４の原理に基づいて構成されるキーシステムで、デバイスのキーとコンテンツのキーの管理が行われる。図５の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、或いは、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの１つのノードに、利用権を管理するシステムとして本システム（適宜、Ｔシステムと称する）が対応する。

【００３７】すなわち、Ｔシステムのノードよりさらに下の階層の２４段のノードに対応するキーにより、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスが対応される。従って、図５の例においては、2^{24}（約１６メガ）のサービスプロバイダ、あるいはサービスを規定することができる。また、最下段の３２段の階層により、2^{32}（約４ギガ）のユーザ（クライアント１）を規定することができる。最下段の３２段のノードからＴシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【００３８】コンテンツを暗号化したコンテンツキーは更新されたルートキーKR'によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB（Enabling Key Block：有効化キーブロック）（図７を参照して後述する）内に配置される。

【００３９】EKBにおける末端から１つ上の段の更新ノードキーはEKBの末端のノードキーあるいはリーフキーによって暗号化され、EKB内に配置される。クライアント１は、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツとともに配布されるEKBに記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たノードキーを用いて、EKBに記述されている、さらにその上の階層の更新ノードキーを復号する。同様の処理を順次行うことで、クライアント１は、更新ルートキーKR'を得ることができる。サービスデータは、クライアント１についての情報を登録したときにライセンスサーバ４から供給されるものであり、このサービスデータと、後述する、特定のコンテンツの利用を許可する情報である利用権の組み合わせをライセンスと呼ぶ。

【００４０】図６は、階層ツリー構造のカテゴリの分類の具体的な例を示す図である。

【００４１】図６において、階層ツリー構造の最上段には、ルートキーKR２３０１が設定され、以下の中間段にはノードキー２３０２が設定され、最下段には、リーフキー２３０３が設定される。各デバイスは、個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーからなるデバイスノードキー（DNK）を保有する。

【００４２】最上段から第M段目（図５の例では、M＝８）の所定のノードがカテゴリノード２３０４として設定される。すなわち、第M段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第M段の１つのノードを頂点としてM＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【００４３】例えば、図６の第M段目の１つのノード２３０５にはカテゴリ［メモリスティック（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード２３０５以下が、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【００４４】M段から数段分下位の段をサブカテゴリノード２３０６として設定することができる。図６の例では、カテゴリ［メモリスティック］ノード２３０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノード２３０６が設定されている。また、サブカテゴリノードである再生専用器のノード２３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード２３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［PHS］ノード２３０８と、［携帯電話］ノード２３０９が設定されている。

【００４５】カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えば、あるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、或いは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。

【００４６】例えば、１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定することにより、メーカーの販売するゲーム機器XYZに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することができ、その後、その頂点ノードキー以下のノードキー、リーフキーによって構成されるEKBを生成して配信することで、暗号化コンテンツの配信処理、各種キーの配信処理、更新処理等を、頂点ノード以下のデバイス（ゲーム機器XYZ）に対してのみ行うことができる。

【００４７】すなわち、頂点ノードに属さない、他のカテゴリのノードに属するデバイスには全く影響を及ぼすことなく、キーの更新等を実行することができる。

【００４８】また、ある時点tにおいて、デバイス３の所有する鍵Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキーＫ００１，Ｋ００，Ｋ０，KRを、それぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）ｔの更新キーであることを示す。

【００４９】更新キーの配布処理ついて説明する。キーの更新は、例えば、図７に示されるEKBによって構成されるテーブルを、ネットワークを介して、あるいは所定の記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、EKBは、図４に示されるようなツリー構造を構成する各リーフ（最下段のノード）に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。

【００５０】図７に示されるEKBは、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図７の例は、図４に示されるツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。

【００５１】図４から明らかなように、デバイス０，１に対しては、更新ノードキーとしてＫ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを提供することが必要であり、デバイス２に対しては、更新ノードキーとしてＫ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを提供することが必要である。

【００５２】図７のEKBに示されるように、EKBには複数の暗号化キーが含まれ、例えば、図７の最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これは、デバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自分自身が有するリーフキーＫ００１０によって、暗号化キーを復号し、更新ノードキーＫ（ｔ）００１を取得できる。

【００５３】また、デバイス２は、復号により得た更新ノードキーＫ（ｔ）００１を用いて、図７の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号することができ、更新ノードキーＫ（ｔ）００を取得することができる。

【００５４】デバイス２は、同様に、図７の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０を取得でき、これを用いて、図７の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒを取得できる。

【００５５】一方、ノードキーＫ０００は、更新する対象のキーに含まれておらず、ノード０，１が更新ノードキーとして必要なのは、Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒである。

【００５６】ノード０，１は、デバイスキーＫ００００，Ｋ０００１を用いて、図７の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号することにより更新ノードキーＫ（ｔ）００を取得し、同様に、順次、図７の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０を取得し、さらに、図７の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒを取得する。このようにして、デバイス０，１，２は、更新したキーＫ（ｔ）Ｒを得ることができる。

【００５７】なお、図７のインデックスは、図の右側に示される暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００５８】図４に示されるツリー構造の上位段のノードキーＫ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図８のEKBを用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００５９】図８に示されるEKBは、例えば、特定のグループにおいて共有される新たなコンテンツキーを配布する場合に利用可能である。

【００６０】例えば、図４の一点鎖線で示されるグループ内のデバイス０，１，２，３が、ある記録媒体を用いており、それらのデバイスに対して新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを設定することが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００により、新たな共通の更新コンテンツキーＫ（ｔ）ｃｏｎが暗号化されたデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）が、図８に示されるEKBとともに配布される。この配布により、デバイス４など、その他のグループの機器が復号す

ることができないデータとしての配布が可能となる。

【００６１】すなわち、デバイス０，１，２は、EKBを処理して得たキーＫ（ｔ）００を用いて暗号データを復号することで、ｔ時点におけるコンテンツキーＫ（ｔ）ｃｏｎを得ることができる。

【００６２】図９は、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理の例として、Ｋ（ｔ）００により新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが暗号化されたデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と、図８に示されるEKBが、所定の記録媒体を介して提供されたデバイス０の処理を模式的に示す図である。すなわち、図９の例は、EKBによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００６３】図９に示されるように、デバイス０は、記録媒体に格納されている世代t時点のEKBと、自分自身に予め用意されているノードキーＫ０００を用いて、上述したようなEKB処理（鍵を順次解く処理）により、ノードキーＫ（ｔ）００を生成する。また、デバイス０は、復号した更新ノードキーＫ（ｔ）００を用いて、更新コンテンツキーＫ（ｔ）ｃｏｎを復号し、それを後に使用するために、自分だけが有するリーフキーＫ０００００で、更新コンテンツキーＫ（ｔ）ｃｏｎを暗号化して格納する。

【００６４】図１０は、EKBのフォーマットの例を示す図であり、このような各種の情報からなるEKBが、コンテンツデータのヘッダに含まれる。

【００６５】バージョン６１は、EKBのバージョンを示す識別子である。このバージョン６１は、最新のEKBを識別する機能と、コンテンツとの対応関係を示す機能を有する。デプス６２は、EKBの配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６３は、EKB中のデータ部６６の位置を示すポインタであり、タグポインタ６４および署名ポインタ６５は、タグ部６７および署名６８の位置をそれぞれ示すポインタである。

【００６６】データ部６６には、例えば、更新するノードキーが暗号化されて得られたデータが格納される。例えば、図９に示されるような、更新されたノードキーに関する各暗号化キー等がデータ部６６に格納される。

【００６７】タグ部６７は、データ部６６に格納された、暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを、図１１を参照して説明する。

【００６８】図１１の例においては、送付されるデータは、図１１Ｂに示されるように、図７の暗号化キーとされている。なお、暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。

【００６９】この例においては、ルートキーの更新キーＫ（ｔ）Ｒが含まれているため、トップノードアドレスはKRとなる。このとき、例えば、最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図１１Ａに示す階層ツリーに示す位置Ｐ０に対応する。次の段のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左下の位置Ｐ００に対応する。

【００７０】すなわち、ツリー構造の所定の位置から見て、その下にデータがある場合には、タグが０に設定され、データがない場合には、タグが１に設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。

【００７１】図１１Ｂの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）に対応する位置Ｐ０の左下の位置Ｐ００にはデータがあるため、Ｌタグ＝０となり、位置Ｐ０の右下にはデータがないため、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図１１Ｃに示すデータ列、およびタグ列が構成される。

【００７２】タグは、対応するデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）が、ツリー構造のどこに位置しているのかを示すために設定される。データ部６６に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）・・・は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによって、データとして格納された暗号化キーのツリー上の位置が判別可能となる。タグを用いずに、図７または図８に示されるように、暗号化データに対応させたノード・インデックスを用いて、例えば、０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（ｔ）００）・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とした場合、そのデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、以上のようなタグを、キーの位置を示す索引データとして用いることにより、より少ないデータ量で、キーの位置の判別が可能となる。

【００７３】図１０の説明に戻り、署名（Signature）６８は、EKBを発行した、例えば、鍵管理センタ（ライセンスサーバ４）、コンテンツプロバイダ（コンテンツサーバ３）、決済機関（課金サーバ５）等が実行する電子署名である。EKBを受領したデバイスは、EKBに含まれる署名を検証することにより、取得したEKBが、正当な発行者が発行したEKBであるか否かを判定する。

【００７４】図１２は、以上のような鍵管理システムにおいて、CD８１に記録されているコンテンツが、クライアント１により取り込まれる処理を模式的に示す図である。

【００７５】クライアント１のCPU２１は、所定のプログラムを実行することで構成されるリッピングモジュール９１を制御し、クライアント１に接続されたCD８１に記憶されているコンテンツを取り込ませる。

【００７６】CPU２１は、リッピングモジュール９１により取り込まれたコンテンツに対して、コンテンツID

(CID)、およびクライアント１に対して固有のものとして設定されるID（ユニークID（Uniq ID））を付加し、得られたデータを記憶部２８に記憶させる。このユニークIDは、例えば、所定の桁数からなる乱数であり、コンテンツに付加されたものと同一のユニークIDがクライアント１により保存される。

【００７７】また、CPU２１は、上述した鍵管理システムにおけるサービスとしてのリッピングモジュール９１により取り込まれたコンテンツの利用権を生成する。例えば、リッピングモジュール９１が、それにより取り込まれたコンテンツが３回だけチェックアウトが可能とされるモジュールである場合、３回だけチェックアウトが可能であることを表す使用条件が記述された利用権が生成される。利用権には、コンテンツに対して付加されたコンテンツIDおよびユニークIDも記述され、コンテンツと利用権の対応付けがなされる。

【００７８】以上のようにして取り込まれたコンテンツを再生するとき、再生するクライアントにおいては、利用権により再生が許可されているか否かが判定されるだけでなく、コンテンツに付加されているユニークIDと、そのコンテンツを再生するクライアントのユニークIDが同一であるか否かが判定される。そして、利用権によりコンテンツの再生が許可され、かつ、コンテンツに付加されているユニークIDと、コンテンツを生成するクライアントのユニークIDが同一である場合にのみ、コンテンツの再生処理が行われる。すなわち、コンテンツと利用権のみをコピーなどにより取得したクライアントにおいては、仮に、利用権により再生が許可されている場合であっても、そのコンテンツを再生できないこととなる。

【００７９】以下、コンテンツを取り込み、それを利用するクライアント１の一連の処理について、フローチャートを参照して説明する。

【００８０】始めに、図１３のフローチャートを参照して、コンテンツを取り込むクライアント１の処理について説明する。

【００８１】例えば、コンテンツが記録されたCD８１（光ディスク４２）などの所定の記録媒体がクライアント１のドライブ３０に装着され、コンテンツを取り込むことが指示されたとき、クライアント１のCPU２１は、所定のプログラムを実行することで構成されるリッピングモジュール９１を制御し、ステップＳ１において、コンテンツを取り込む。

【００８２】CPU２１は、ステップＳ２において、コンテンツを識別するコンテンツIDを生成する。また、CPU２１は、ステップＳ３において、クライアント１（リッピングモジュール９１）に対して固有のユニークIDが、例えば、記憶部２８に記憶されているか否かを判定し、それが記憶されていないと判定した場合、ステップＳ４に進み、所定の桁数からなるユニークIDを生成する。生成されたユニークIDは、記憶部２８に保存される。

【００８３】なお、ユニークIDとして、クライアント１において生成されたものではなく、例えば、クライアント１のユーザが、リッピングモジュール９１を利用可能なものにするべく、所定の情報をライセンスサーバ４に登録したときに、ライセンスサーバ４からクライアント１に付与されるものを使用するようにしてもよい。このようにしてユニークIDが付与された場合、または、過去に行われたリッピングにおいて既に生成されている場合、図１３のステップＳ３において、ユニークIDがあると判定され、ステップＳ４の処理がスキップされる。

【００８４】CPU２１は、ステップＳ５において、コンテンツIDおよびユニークIDを、コンテンツの所定の属性情報が記述される領域としての「Attribute（属性）」に記述する。コンテンツのフォーマットについては後に詳述する。

【００８５】ステップＳ６において、CPU２１は、属性情報として記述されている情報に基づいたデジタル署名を、自分自身の秘密鍵を用いて作成する。この秘密鍵は、例えば、クライアント１に関する情報を登録したときにライセンスサーバ４から提供されたものである。

【００８６】ステップＳ７において、CPU２１は、コンテンツに対応して記録するヘッダのデータを作成する。ヘッダのデータは、コンテンツID、利用権ID、利用権を取得するためのアクセス先を表すURL、およびウォーターマークにより構成される。

【００８７】CPU２１は、ステップＳ８において、自分自身の秘密鍵を用いて、ステップＳ７の処理で作成したヘッダのデータに基づいたデジタル署名を作成する。CPU２１は、ステップＳ９において、暗号化復号部２４を制御し、生成したコンテンツキーでコンテンツを暗号化させる。生成されたコンテンツ、およびそれに付随するヘッダなどの情報は、ステップＳ１０において、記憶部２８に保存される。

【００８８】図１４は、コンテンツのフォーマットの例を示す図である。

【００８９】図１４に示されるように、コンテンツは、ヘッダ、EKB、コンテンツキーＫｃをルートキーＫｒｏｏｔで暗号化して得られるデータ（Enc（Ｋｒｏｏｔ，Ｋｃ））、コンテンツIDおよびユニークIDが記述される属性情報（Attribute）、証明書（Cert）、ヘッダに基づいて生成されたデジタル署名（Sig（Header））、コンテンツをコンテンツキーＫｃで暗号化して得られるデータ（Enc（Ｋｃ，Content））、メタデータ（Meta Data）、およびマーク（Mark）から構成される。

【００９０】ヘッダには、コンテンツID（CID）、コンテンツに対応する利用権を識別する利用権ID（利用権ID）、利用権の取得先（クライアント１）を表すURL、およびウォーターマーク（WM）が記述されている。

【００９１】コンテンツの属性には、コンテンツID、コンテンツの提供者を識別するための識別情報としてのレ

コードカンパニーID、アーティストを識別するための識別情報としてのアーティストID、および、ユニークIDなどが含まれる。本実施例では、属性は利用権の対象となるコンテンツを特定するために用いられる。

【００９２】なお、メタデータは、コンテンツに関連する各種の情報であり、例えば、音楽コンテンツに対しては、ジャケット、写真、歌詞等のデータがメタデータとしてコンテンツに付加される。また、マークには、ユーザのID（リーフID）、所有権フラグ、使用開始時刻、コピー回数、これらの情報に基づいて生成されたデジタル署名が記述される。マークの所有権フラグは、例えば、所定の期間だけコンテンツを使用可能とする利用権を、そのまま買い取ったような場合（使用期間を永久に使用できるのものに変更したような場合）に付加される。また、マークのコピー回数には、そのコンテンツをコピーした回数などの履歴（ログ）が記述される。

【００９３】以上においては、コンテンツがCD８１から取得（リッピング）される場合について説明したが、例えば、インターネット２を介して所定のサーバから取得されたコンテンツなどについても、同様に、コンテンツIDとともにクライアント１のユニークIDが付加されて、クライアント１により保存される。

【００９４】次に、図１５のフローチャートを参照して、取り込まれたコンテンツに対応する利用権を生成するクライアント１の処理について説明する。

【００９５】ステップＳ２１において、リッピングモジュール９１により取り込まれたコンテンツに対して付与するものとして予め設定されている利用権を、図１３の処理により取り込まれたコンテンツに対応する利用権として記憶部２８から読み出す。記憶部２８に記憶されている利用権には、利用権ID、バージョン、作成日時、有効期限等の情報が記述されている。

【００９６】ステップＳ２２において、CPU２１は、選択した利用権にユニークIDを付加するとともに、コンテンツの属性情報として記述されているユニークIDと同一のIDが設定されているクライアント１においてのみ、そのコンテンツを再生できることを表す情報を付加する。また、CPU２１は、ステップＳ２３において、使用条件を選択し、それを付加する。例えば、リッピングモジュール９１に対して、それにより取り込まれたコンテンツが同時に３回だけチェックアウトできることが設定されている場合、３回だけチェックアウトできることを表す使用条件が選択される。また、例えば、リッピングモジュール９１に対して、それにより取り込まれたコンテンツが自由にコピーできることが設定されている場合、それを表す使用条件が選択される。

【００９７】CPU２１は、ステップＳ２４において、以上のようにして選択した利用権に記述されているデータのデジタル署名を作成し、それを付加する。デジタル署名が付加された利用権は、ステップＳ２５において、記憶部２８に保存される。

【００９８】図１６は、利用権のフォーマットの例を示す図である。

【００９９】バージョンは、メジャーバージョンおよびマイナーバージョンをドットで区切って、利用権のバージョンを記述する情報である。プロファィルは、１０進の整数値から記述され、利用権の記述方法に対する制限を規定する情報である。利用権IDは、１６進定数で記述される、利用権を識別するための識別情報である。作成日時は、利用権が作成された日時を示す。有効期限は、利用権の有効期限を示す。９９９９年２３時５９分５９秒である有効期限は、有効期限に制限がないことを示す。使用条件には、その利用権に基づいて、コンテンツを使用することが可能な使用期限、その利用権に基づいて、コンテンツを再生することが可能な再生期限、コンテンツの最大再生回数、その利用権に基づいて、コンテンツをコピーすることが可能な回数（許されるコピー回数）、最大チェックアウト回数、その利用権に基づいて、コンテンツをCD-Rに記録することができるか否か、PD（Portable Device）にコピーすることが可能な回数、利用権の移動の可否、使用ログをとる義務の有無等を示す情報が含まれる。使用条件の電子署名は、使用条件に対応する電子署名である。

【０１００】定数は、使用条件または使用状態で参照される定数である。ユニークIDは、コンテンツを取り込むときに生成されたものである。電子署名は、利用権全体に対応する、電子署名である。証明書は、ライセンスサーバ４の公開鍵を含む証明書である。

【０１０１】また、クライアント１の記憶部２８には、利用権の使用条件とあわせて、コンテンツや利用権の状態を表す情報である使用状態（コンテンツ条件）が記憶される。使用状態には、対応する利用権に基づいてコンテンツを再生した回数、コンテンツをコピーした回数、コンテンツをチェックアウトした回数、コンテンツを初めて再生した日時、コンテンツをCD-Rに記録した回数、その他コンテンツあるいは利用権に関する履歴情報等を示す情報が含まれる。コンテンツの再生の条件の判定は、利用権に含まれる使用条件と、記憶部２８に利用権と共に記憶されている使用状態とを基に行われる。例えば、使用状態に記憶されているコンテンツを再生した回数が、使用条件に含まれるコンテンツ最大再生回数より少ない場合には、再生の条件が満たされていると判定される。

【０１０２】次に、図１７のフローチャートを参照して、リッピングモジュール９１によりコンテンツを取り込んだクライアント１による、コンテンツの再生処理について説明する。

【０１０３】ステップＳ４１において、クライアント１のCPU２１は、ユーザが入力部２６を操作することで指示したコンテンツをコンテンツIDに基づいて記憶部２８

から読み出し、読み出したコンテンツの属性情報として記述されているユニークIDを読み取る。また、CPU２１は、ステップＳ４２において、再生が指示されたコンテンツに対応する利用権を利用権IDに基づいて読み出し、読み出した利用権に記述されているユニークIDを読み取る。

【０１０４】ステップＳ４３において、CPU２１は、保存しておいたユニークID、すなわちクライアント１のユニークIDを記憶部２８から読み出し、ステップＳ４４に進み、それらのユニークID、すなわち、コンテンツに記述されているユニークID、利用権に記述されているユニークID、およびクライアント１に保存されているユニークIDが全て同じであるか否かを判定する。なお、コンテンツに記述されているユニークIDと、クライアント１に保存されているユニークIDのみが同一であるか否かが判定されるようにしてもよい。

【０１０５】CPU２１は、ステップＳ４４において、全てのユニークIDが同一であると判定した場合、ステップＳ４５に進み、利用権により、コンテンツの使用が許可されているか否かを、記述されている使用条件に基づいて判定する。例えば、CPU２１は、利用権の記述内容としての有効期限（図１６参照）と、タイマ２０により計時されている現在日時を比較することにより、利用権が有効期限内のものであるか否か、すなわち、コンテンツの使用が許可されているか否かを判定する。

【０１０６】ステップＳ４５において、利用権により使用が許可されていると判定された場合、ステップＳ４６に進み、CPU２１は、RAM２３に記憶された（読み出された）コンテンツを復号する処理を実行する。ステップＳ４６において行われるコンテンツ復号処理については、図１８のフローチャートを参照して後述する。

【０１０７】CPU２１は、ステップＳ４７において、暗号化復号部２４により復号されたコンテンツをコーデック部２５に供給し、デコードさせる。そして、CPU２１は、コーデック部２５によりデコードされたデータを、入出力インタフェース３２を介して出力部２７に供給し、ディジタルアナログ変換させ、スピーカから出力させる。

【０１０８】なお、ステップＳ４４で、コンテンツに記述されているユニークIDと、クライアント１に保存されているユニークID（さらに、利用権に記述されているユニークID）が異なると判定された場合、並びに、ステップＳ４５で、利用権によりコンテンツの再生が許可されていないと判定された場合、ステップＳ４８において、エラー処理が行われ、その後、処理が終了される。

【０１０９】次に、図１８のフローチャートを参照して、図１７のステップＳ４６において実行されるクライアントの復号処理の詳細について説明する。

【０１１０】ステップＳ６１において、クライアント１のCPU２１は、サービスデータに含まれてライセンスサーバ４から提供されたDNKにより、EKBに含まれる鍵情報を順次復号し、ルートキーＫｒｏｏｔ（KR）を取得する。CPU２１は、ルートキーＫｒｏｏｔを取得したとき、ステップＳ６２に進み、ルートキーＫｒｏｏｔを用いてコンテンツキーＫｃを復号する。図１４に示されるように、コンテンツには、コンテンツキーＫｃがルートキーＫｒｏｏｔにより暗号化されて得られたデータＥｎｃ（Ｋｒｏｏｔ，Ｋｃ）が付加されている。

【０１１１】ステップＳ６３において、CPU２１は、ステップＳ６２で取得したコンテンツキーＫｃによりコンテンツを復号する。

【０１１２】図１９は、以上の復号処理を模式的に表したものである。なお、図１９においては、コンテンツはクライアント１により保存されていたものであり、図１４に示される情報のうち、主な情報のみが示されている。

【０１１３】すなわち、ライセンスサーバ４からクライアント１に提供されたDNKに基づいて、EKBからルートキーＫｒｏｏｔが取得され（図１８のステップＳ６１）、取得されたルートキーＫｒｏｏｔにより、データＥｎｃ（Ｋｒｏｏｔ，Ｋｃ）が復号され、それによりコンテンツキーＫｃが取得される（図１８のステップＳ６２）。そして、コンテンツキーＫｃにより、データＥｎｃ（Ｋｃ，Content）が復号され、コンテンツ（Content）が取得される（図１８のステップＳ６３）。なお、図１４および図１９のEKBには、図２０に示されるように、ルートキーＫｒｏｏｔがDNKにより暗号化されて得られたデータＥｎｃ（DNK，Ｋｒｏｏｔ）が含まれている。

【０１１４】以上のようにしてコンテンツの再生を制御することにより、コンテンツとともに、利用権を不正に取得したクライアント（ユニークIDが管理されていないクライアント）であっても、コンテンツを再生できないこととなる。

【０１１５】また、以上の処理によりクライアント１により取り込まれたコンテンツがチェックアウトが可能であるとされている場合（チェックアウト可能であることが使用条件として設定されている場合）、クライアント１からコンテンツのチェックアウトを受ける他のクライアントに対しては、コンテンツ、利用権、およびクライアント１のユニークIDが所定の方法により暗号化されて提供されるようにしてもよい。その場合、それらの情報の提供を受けたクライアントにおいては、図１７および図１８に示されるものと同様の処理が実行され、コンテンツの再生が行われる。これにより、コンテンツが最初に取り込まれたクライアント１の管理下でのコンテンツのチェックアウト／チェックイン等が行われる。

【０１１６】また、上記実施例では、コンテンツを利用するために必要な利用権を特定するためにコンテンツの属性と利用権のコンテンツ条件を用いたが、これに限らない。例えば、コンテンツに、該コンテンツを利用する

ために必要な利用権の利用権IDを含むようにしても良く、この場合、コンテンツを指定すればそれを利用するために必要な利用権は一意に決まるため、両者のマッチングを決定する処理を行う必要はない。

【0117】

【発明の効果】本発明によれば、コンテンツを提供することができる。

【0118】また、本発明によれば、不正なコンテンツの利用を防止することができる。

【図面の簡単な説明】

【図1】従来のコンテンツの管理システムの模式図である。

【図2】本発明を適用したコンテンツ提供システムの構成例を示す図である。

【図3】図2のクライアントの構成例を示すブロック図である。

【図4】キーの構成を示す図である。

【図5】カテゴリノードを示す図である。

【図6】ノードとデバイスの対応例を示す図である。

【図7】有効化キーブロックの構成例を示す図である。

【図8】有効化キーブロックの他の構成例を示す図である。

【図9】有効化キーブロックの利用を模式的に表した図である。

【図10】有効化キーブロックのフォーマットの例を示す図である。

【図11】有効化キーブロックのタグの構成を説明する図である。

【図12】本発明を適用したコンテンツの管理システムの模式図である。

【図13】図1のクライアントのコンテンツ取り込み処理を説明するフローチャートである。

【図14】コンテンツのフォーマットの例を示す図である。

【図15】図1のクライアントの利用権生成処理を説明するフローチャートである。

【図16】利用権のフォーマットの例を示す図である。

【図17】図1のクライアントのコンテンツ再生処理を説明するフローチャートである。

【図18】図17のステップS46における復号処理の詳細を説明するフローチャートである。

【図19】図18の復号処理を模式的に表した図である

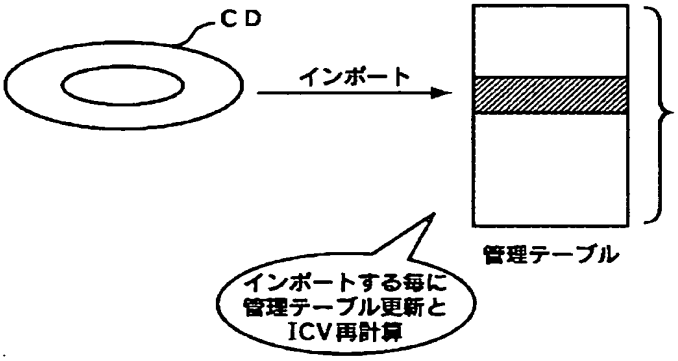
【図20】図19のEKBに含まれる情報の例を示す図である。

【符号の説明】

1-1，1-2 クライアント， 2 インターネット， 3 コンテンツサーバ， 4 ライセンスサーバ， 5 課金サーバ， 20 タイマ， 21CPU， 24 暗号化復号部， 25 コーデック部， 26 入力部， 27出力部， 28 記憶部， 29 通信部

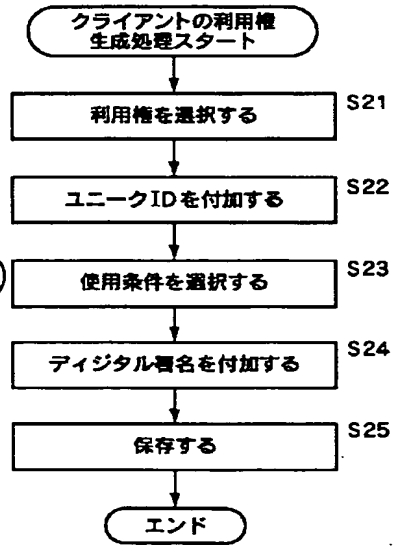
【図1】

図1



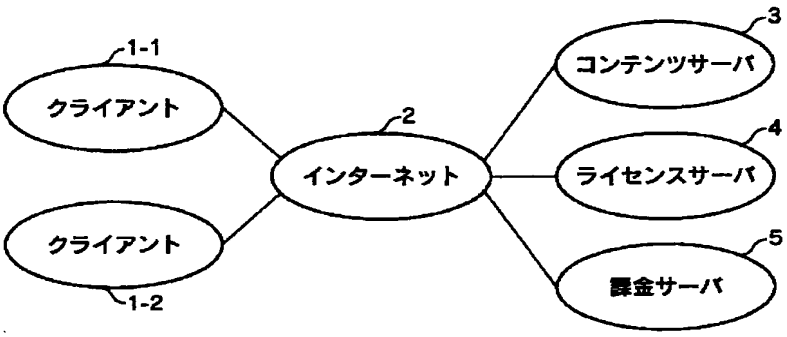
【図15】

図15



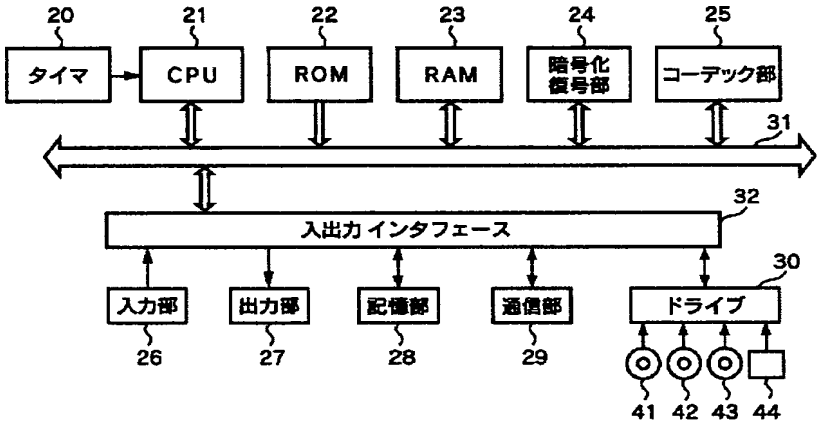
【図2】

図2



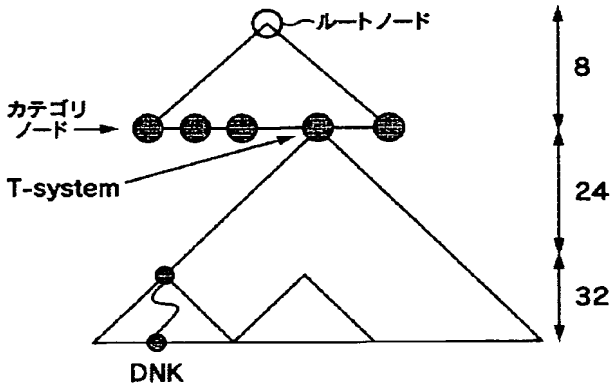
【図3】

図3



【図5】

図5



【図16】

図16

バージョン
プロファイル
利用権ID
作成日時
有効期限
使用条件
コンテンツ条件
定数
ユニークID
署名
証明書

【図20】

図20

EKB

Enc(DNK, Kroot)

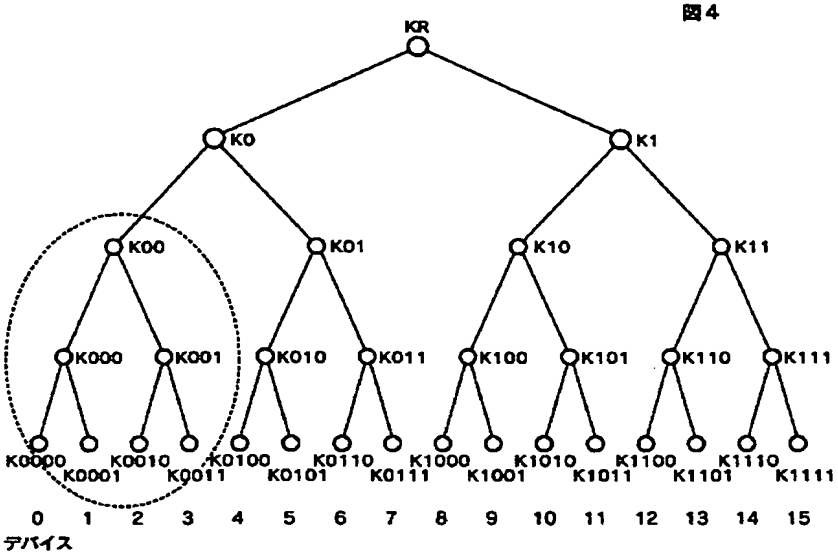
【図7】

図7

バージョン(Version) :t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

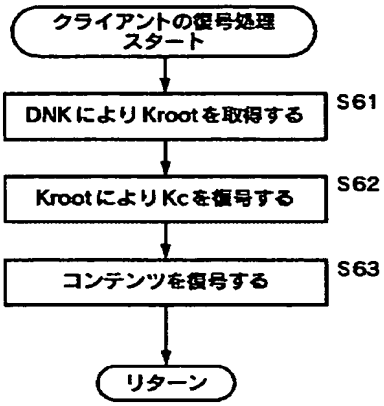
【図4】

図4



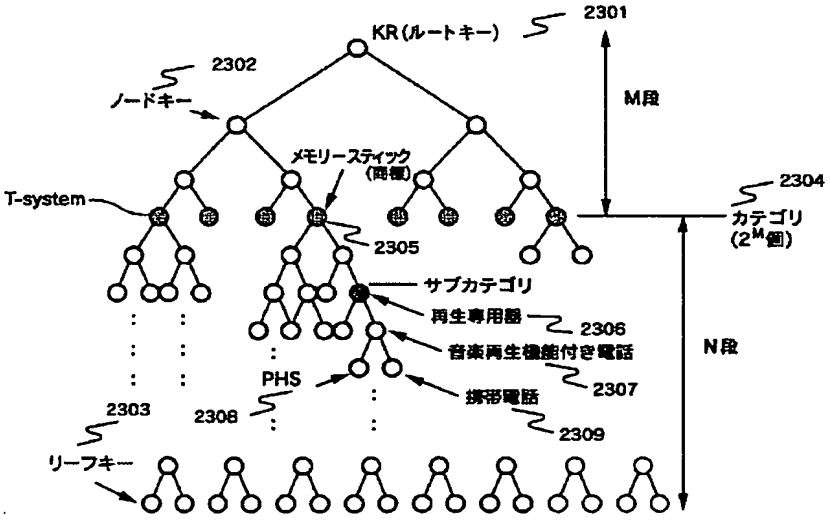
【図18】

図18



【図6】

図6



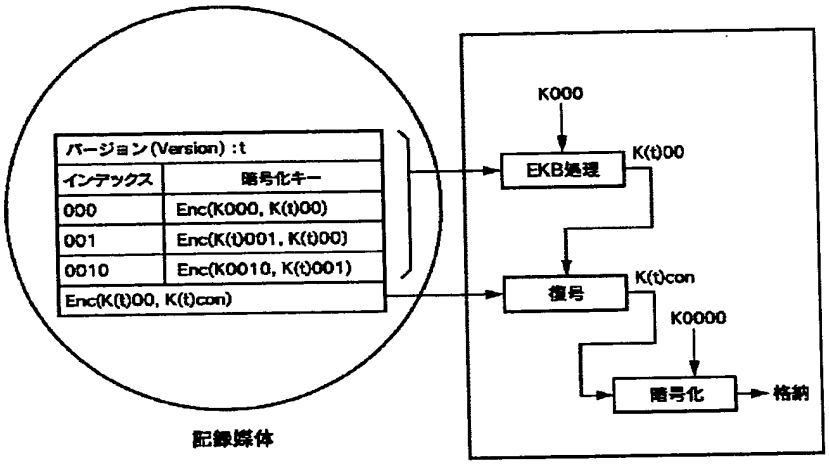
【図8】

図8

バージョン(Version) :t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

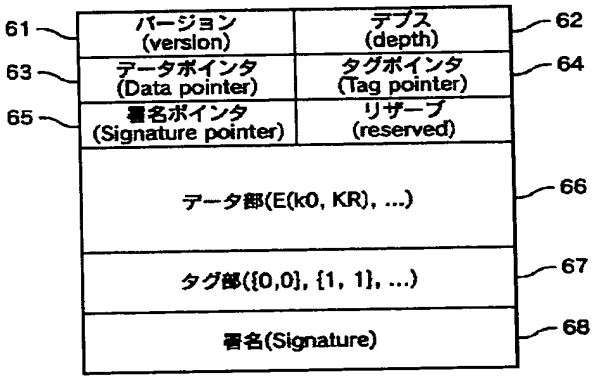
【図9】

図9



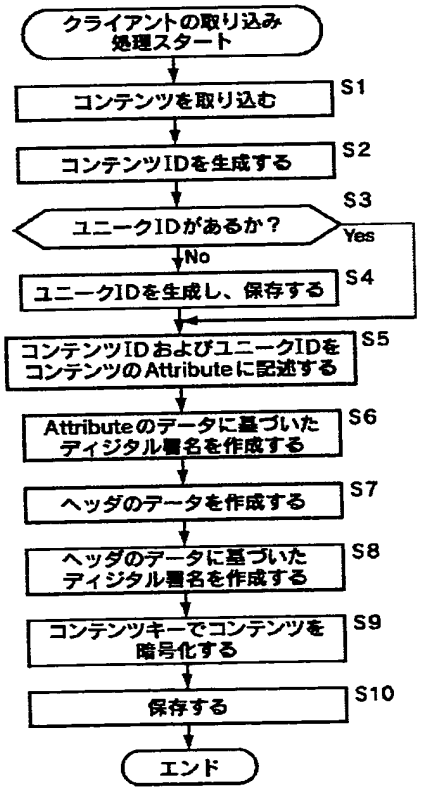
【図10】

図10



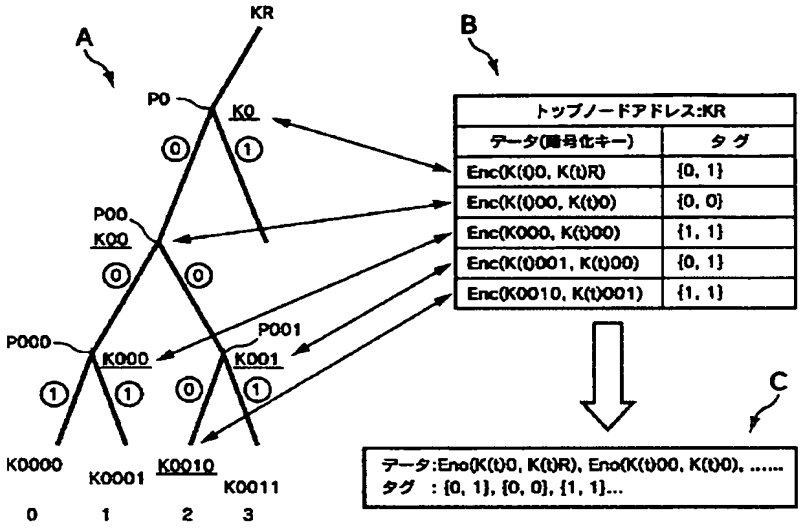
【図13】

図13



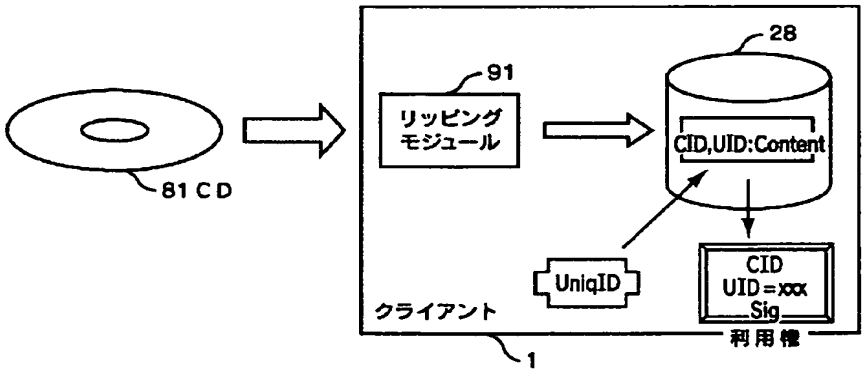
【図11】

図11



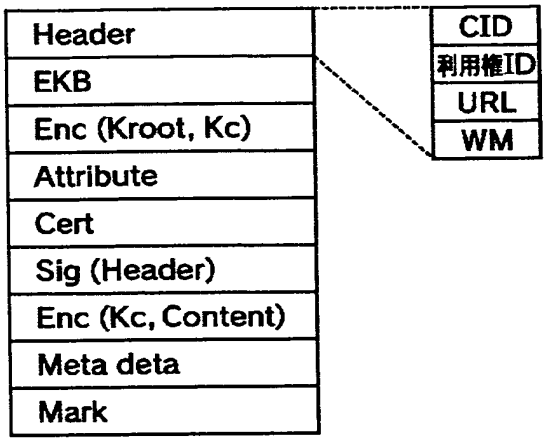
【図12】

図12



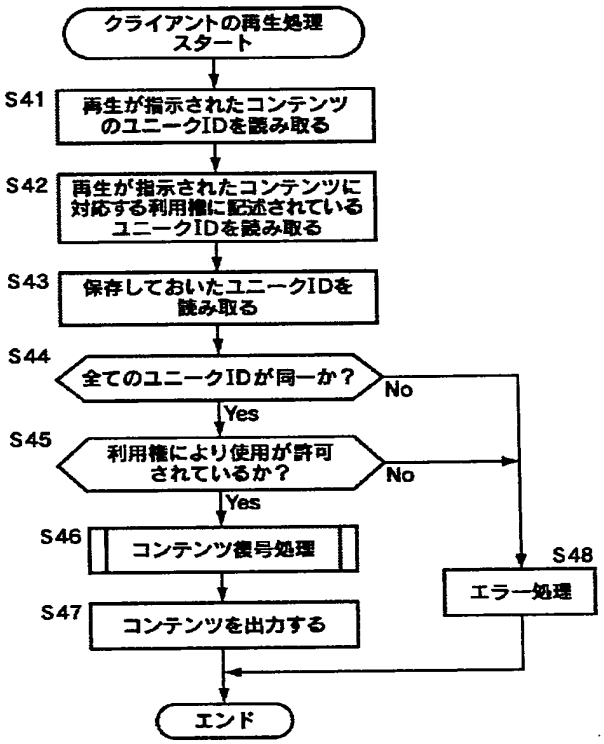
【図14】

図14



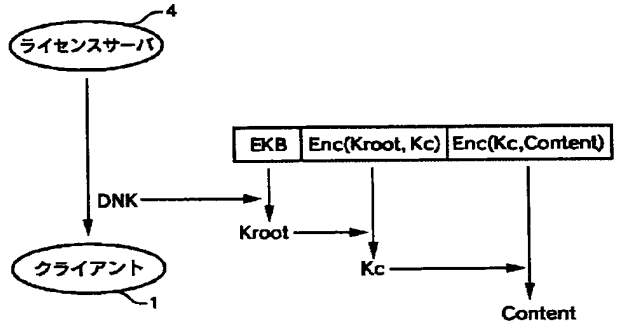
【図17】

図17



【図19】

図19



フロントページの続き

(72)発明者　江面　裕一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　長野　元彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Fターム(参考) 5B017 AA06 BB09 BB10 CA16
5B085 AE00 BA06 BG03 BG04 BG07
5C064 BA01 BB01 BB02 BC01 BC16
CB01 CC04
5D044 AB05 AB07 BC01 BC03 CC04
DE49 DE50 DE54 FG18 GK12
GK17 HH15 HL02 HL08 HL11